Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)	
JRL-3995-42 **Confirmation No. 4649**	

Application Number	Filed
10/530,293	April 5, 2005
First Named Inventor	
NÄSLUND	
Art Unit	**Examiner**
2435	Schwartz, Darren B.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

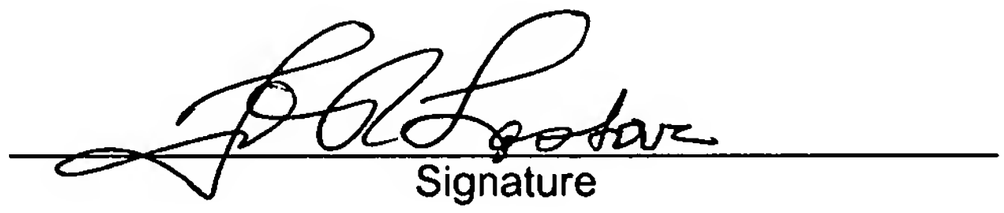
I am the

☐ Applicant/Inventor

☐ Assignee of record of the entire interest. See 37 C.F.R. § 3.71. Statement under 37 C.F.R. § 3.73(b) is enclosed. (Form PTO/SB/96)

☒ Attorney or agent of record 33,149 (Reg. No.)

☐ Attorney or agent acting under 37CFR 1.34.
Registration number if acting under 37 C.F.R. § 1,34 _____


Signature

John R. Lastova
Typed or printed name

703-816-4025
Requester's telephone number

July 21, 2010
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.*

☒ *Total of 1 form/s are submitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

NASLUND et al.

Atty. Ref.: 3995-42; Confirmation No. 4649

Appl. No. 10/530,293

TC/A.U. 2435

Filed: April 5, 2005

Examiner: Schwartz, Darren B.

For: SECURITY AND PRIVACY ENHANCEMENTS FOR SECURITY DEVICES

* * * * * * * * * * *

July 21, 2010

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Claims 44, 46, 49-59, 61, and 79-82 stand rejected under 35 USC §103(a) as being unpatentable based on a Wireless Identity Module protocol document referred to by the Examiner as WIM in view of Ogasawara and further in view of newly-cited Aura (USP 6,711,400). This rejection is respectfully traversed.

WIM describes a tamper-resistant security device with a memory for storing user credentials like a security key and an AKA-module for performing AKA processing with the security key. WIM defines an interface between part of a WAP client device and the tamper-resistant security device, i.e., WIM defines an **external** interface to the security device. Page 63 of the WIM-document discloses a card (mapped to a tamper-resistant security device) incorporating a WIM-application and other applications so that these applications are protected and executed in a tamper-resistant environment. But there is no disclosure in WIM of an **internal** interface between the other applications or the WIM-application and the AKA-module. Input to and output from the WIM-application and the other applications are directed over the external interface to the tamper-resistant security device for processing by the WIM-application or other applications.

Nor does WIM disclose the claimed cooperating application or its post processing, as the Examiner agrees. The Examiner relies on Ogasawara as allegedly teaching the cooperating

application and the claimed internal interface and on Aura as allegedly teaching the post processing. Applicants respectfully disagree.

Ogasawara discloses a system for controlling access to one or more data fields in an IC card connected to a terminal (Fig. 2). A user selects a data field for access and provides a personal identification number (PIN) and an authentication code (AC) corresponding to the data field. The IC card verifies the PIN and AC and allows access to the field. The Examiner contends that Ogasawara's IC card generic "control program" stored in ROM is the claimed "cooperating program" to permit access to a data field area in the IC.

For the claimed internal interface that allows cooperative processing between a cooperating application and the AKA module (both of which are wholly contained within the tamper security device), the Examiner refers to col. 2, lines 43-45, which discloses that "the circuit of the IC card can communicate with the program portion in the terminal apparatus." It is clear in Figure 2 that the terminal apparatus is external to the IC card which is being mapped by the Examiner to the tamper-resistant security device used in a user device.

If the pre-appeal panel maintains the final rejection, Applicants request identification of the specific structure or feature in Ogasawara that the panel contends corresponds to the claimed (1) AKA module, (2) internal interface, (3) AKA process command, and (4) enhanced security processing performed by the cooperating application in conjunction with the AKA module of an ongoing authentication and key agreement process being performed by the AKA module. This identification is needed because the column/line references in the final action are ambiguous and unclear. This will allow Applicants to know the basis of the rejection and permit a more focused appeal.

Once Ogasawara confirms the PIN and AC, the requested access to the data field is allowed, and data may be provided to the user which ends the entire process. In contrast, claim 44 recites that "said enhanced security processing by said cooperating application includes post-processing of at least one AKA output parameter produced by the AKA module in response to the one or more AKA process commands, said post-processing including encapsulation of said at least one AKA output parameter to generate a further AKA parameter that has higher security than said at least one AKA output parameter produced in response to the one or more AKA process commands." The Examiner admits this quoted language is missing from both WIM and Ogasawara and turns to a third reference--Aura.

Aura relates to an authentication method that spans between a mobile station (MS), a visited public land mobile network (VPLMN), and an HLR/AUC node as shown in Figure 4. The Examiner seems to contend that Aura's processing in the HLR/AUC node of the mobile identifier IMSI and RAND1 in Figure 4 to retrieve Ki, generate RAND2, and perform one-way hash functions H1-H3 in block 405 to generate SRES1, SRES2', and Kc corresponds to the claimed enhanced security processing. But, even assuming this were the case, the enhanced security processing would be performed in a separate node HLR/AUC that is quite remote from the MS and its SIM. In other words, under this assumption, Aura's enhanced processing is occurring outside of a tamper-resistant security device, (which is the SIM card in Aura's MS), rather than "contained within the tamper-resistant security device," as claimed. Indeed, it is occurring outside of the mobile station (MS) and across an entire visiting network in the remote authentication node HLR/AUC.

But the assumption is also wrong. Blocks 405 and 407 are AKA modules in the HLR/AUC and MS, respectively. Neither block can be the claimed cooperating application because neither cooperates with an existing AKA module nor operates on outputs of the AKA module.

Unlike what is claimed, Aura's teachings are directed to replacing the normal GSM AKA module with a different, replacement AKA module. Specifically, in the conventional GSM AKA module that Aura is trying to improve, an internally-stored key Ki and a received random number RAND are used to generate RES and Kc using functions called A3 and A8. The conventional GSM AKA module is defined by these functions A3 and A8. Aura simply replaces the two A3 and A8 functions with three H1, H2, and H3 functions as is shown in blocks 405 and 407. This can also be seen by comparing Figs. 3 and 4 side-by-side which makes it is clear that the A3 and A8 AKA functions of Fig. 3 are replaced by the H-functions of Fig. 4. So three H-functions are used instead of two with at least a third function being introduced (assume it is H3) which is not part of the GSM AKA.

Moreover, to compute H1-H3 at the MS, Aura's MS needs direct access to the key Ki, which means that the AKA module 407 must already contain the key Ki as indicated in 407. This is necessary to ensure that the key Ki is not exposed outside of the AKA module for security reasons. Hence, the computations of H1-H3 are not "post-processing of at least one AKA output parameter." It is already established that 405 and 407 are not in the same security device. Each of Aura's blocks 405 and 407 performs a new AKA processing altogether

operating on the inputs each of these blocks receive. To suggest that the claimed post-processing can be performed by another node across a network is the same as post-processing performed within the same security device is untenable and unreasonable.

And as established above, neither block 405 nor block 407 is the claimed "cooperating application" because they are the AKA modules. Since the block 405 is the AKA module in Aura, it is unclear what in the HLR/AUC is performing the claimed post-processing since there is no other block that follows block 405 at the HLR/AUC in Fig. 4. If RAND2, SRES1, SRES2', and Kc are the AKA output parameters, Aura's HLR/AUC does not "generate a further AKA parameter that has higher security than said at least one AKA output parameter."

If the pre-appeal board maintains the final rejection, it is requested that they specifically identify what specific structure or feature in Aura corresponds to the claimed: (1) AKA module, (2) cooperating application, (3) received AKA process command(s), (4) enhanced AKA process command(s), (5) post-processing operation, (6) encapsulation, (7) AKA output parameter, and (8) further AKA parameter because the column/line references in the final action are ambiguous and unclear, this identification will allow Applicants to know the actual basis of the rejection for full appeal.

The Examiner argues it would have been obvious to combine WIM, Ogasawara, and Aura "for the purpose of mutually authenticating two devices and verifying the reliability of the communications network used to authenticate the two devices." This argument is at odds with what the Examiner is using Ogasawara for in the rejection, namely, to allegedly teach a single, self-contained security device. Aura's security approach is to authenticate two devices. So it is unreasonable to try to combine Aura with Ogaswara. Moreover, "verifying the reliability of the communications network used to authenticate the two devices" has no relevance to providing a tamper-resistant security device used in a user device.

Several dependent claim features are also not taught. For example, WIM section 11.3.6.4 simply describes a perform security operation command that "implements all security related APDU commands." It is not seen how this teaches "transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure," as recited in claim 56.

For claims 60 and 62, the Examiner is forced to rely on a fourth reference further evidencing the strained and improper hindsight attempt to reconstruct these claims in the final rejection.

The final rejection should be withdrawn and the case allowed.

Respectfully submitted,
NIXON & VANDERHYE P.C.

By: _____
John R. Lastova
Reg. No. 33,149

901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000